The Polynomial Method and Diophantine Approximation

Edward Young

June 25, 2024

We introduce some important results from the field of diophantine approximation, which asks how well a real number can be approximated by rationals or, more formally, how large $s > 0$ can be for a given $\beta \in \mathbb{R}$ so that

$$\left|\beta - \frac{p}{q}\right| \leq |q|^{-s}$$

has infinitely many integer solutions p, q.

Liouville's theorem 3 is proved by a simple argument using an auxiliary polynomial, this then motivates the proof of Thue's theorem 7 which is the topic of the next talk.

In the remainder of the talk, we look at diophantine equations and how Thue's theorem bounds the number of their solutions.

This talk follows the first part of [2, Chapter 16].

1 Diophantine Approximation

Proposition 1 (Dirichlet)**.** *For any irrational number $\beta \in \mathbb{R}$, there are infinitely many solutions $(p, q) \in \mathbb{Z}^2$ to the inequality*

$$\left|\beta - \frac{p}{q}\right| \leq |q|^{-2}$$

Proof. For $x \in \mathbb{R}$, define $\langle x \rangle = x - \lfloor x \rfloor$ the fractional part of x. For given $Q \in \mathbb{N}$, we divide $[0, 1)$ into Q intervals (pigeon-holes) of length $1/Q$. We have Q numbers $\langle \beta \rangle, \langle 2\beta \rangle ..., \langle Q\beta \rangle \in [0, 1)$, so exist $1 \leq q_1 \neq q_2 \leq Q$ with

$$|\langle q_2\beta \rangle - \langle q_1\beta \rangle| \leq 1/Q$$

Supposing without loss of generality that $\langle q_2\beta\rangle > \langle q_1\beta\rangle$, we have

$$|\langle q_2\beta\rangle - \langle q_1\beta\rangle| = \langle (q_2 - q_1)\beta\rangle \leq 1/Q$$

Setting $q = q_2 - q_1, p = \lfloor q\beta \rfloor$

$$|q\beta - p| \leq 1/Q$$

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{qQ} \leq q^{-2}$$

Q was arbitrary $\Rightarrow$ infinitely many solutions $(p, q) \in \mathbb{Z}^2$ in total. □

Remark 2. On the other hand, for $s > 2$, the set $D_s = \left\{\beta \in \mathbb{R} : \left|\beta - \frac{p}{q}\right| \leq |q|^{-s} \text{ has } \infty \text{ solutions}\right\}$ has measure 0:

$$A_s(p, q) = \left\{\beta \in [0, 1) : \left|\beta - \frac{p}{q}\right| \leq |q|^{-s}\right\}, \qquad B_s(q) = \bigcup_{p=0}^{q} A_s(p, q)$$

$$D_s \cap [0, 1) = \limsup_{q\to\infty} B_s(q)$$

$$\mu(A_s(p, q)) = 2q^{-s} \Longrightarrow \mu(B_s(q)) \leq \sum_{p=0}^{q} 2q^{-s} \leq 4q^{-s+1}$$

$$\sum_{q} \mu(B_s(q)) < \infty$$

Then $\mu(D_s) = 0$ by the Borel-Cantelli lemma.

Theorem 3 (Liouville, 1844)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree $d > 1$ over $\mathbb{Q}$. Then there exists a constant $C(\alpha) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq C(\alpha) \cdot q^{-d}$$

Proof. a) Find an auxiliary polynomial: Here we use the minimal polynomial m_α of α irreducible over the integers.

b) Vanishing at $\frac{p}{q}$: m_α irreducible, hence $m(p/q) \neq 0$ for any $p/q \in \mathbb{Q}$.

c) Lower Bound: From degree d and integer coefficients, we have $|m(p/q)| \geq 1/q^d$

d) Upper Bound: By Taylor's theorem, if $|\alpha - p/q| \leq 1$ then

$$|m(p/q)| \leq c(\alpha)|\alpha - p/q|$$

e) Compare Bounds: Take $C(\alpha) = \min(1, c(\alpha)^{-1})$. Conclude from c) and d).

□

We now have a complete picture for $d = 2$ but not for larger d. The proof of Theorem 3 is a simplistic example of the method used to prove Thue's theorem, the topic of next week's talk.

The following statements formalise one of the key ideas of the proof, providing the lower bound in step c).

Definition 4. Let $P(x) = \sum a_{i_1,\ldots,i_n} x^{i_1} \cdots x^{i_n} \in \mathbb{R}[x_1, \ldots, x_n]$ a polynomial in finitely many variables, then we define *the norm* of P as

$$|P| = \max |a_{i_1,\ldots,i_n}|$$

Lemma 5 (Gauss)**.** *If $P \in \mathbb{Z}[x]$ satisfies $P^{(j)}(p/q) = 0$ for some rational p/q in lowest terms and every $j = 0, \ldots, k-1$, then $P(x) = (qx - p)^k \cdot \tilde{P}(x)$ for $\tilde{P} \in \mathbb{Z}$.*

In this case, if $P \neq 0$ then $|P| \geq |q|^k$.

Proof. Recall that $P(p/q) = 0 \Rightarrow P(x) = (x - p/q)P_1(x)$. Then if the derivative $P'(x) = (x - p/q)P_1'(x) - P_1(x)$ also has a root at p/q, we find $P_1(x) = (x - p/q)P_2(x)$ which implies $P(x) = (x - p/q)^2 \tilde{P}_2(x)$. Continuing this inductively and factoring out q^k, we get $P(x) = (qx - p)^k \tilde{P}(x)$. It remains to show that this $\tilde{P}$ has integer coefficients.

We clear denominators and factor out common divisors

$$P(x) = \frac{N}{M}(qx - p)\overline{P}(x)$$

$$M \cdot P(x) = N \cdot (qx - p)\overline{P}(x)$$

where now $\overline{P}(x)$ has coprime integer coefficients. Inspecting this modulo prime numbers forces $M = \pm 1$ as needed. □

Proposition 6. *Let $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1) \in \mathbb{Z}[x_1, x_2]$ and $k \geq 2$.*

Suppose $\partial_1^j P(r_1, r_2) := \frac{\partial^j}{\partial x_1^j} P(r_1, r_2) = 0$ for some $(r_1, r_2) \in (p_1/q_1, p_2/q_2) \in \mathbb{Q}^2$ and for all $0 \leq j < k$. then

$$|P| \geq \min \left\{ (2 \deg P)^{-1} q_1^{\frac{l-1}{2}}, q_2 \right\}$$

Proof. Our assumption gives

$$0 = \partial_1^j P(r_1, r_2) = P_1^{(j)}(r_1) r_2 + P_0^{(j)}(r_2) = \begin{pmatrix} P_1^{(j)} \\ P_0^{(j)} \end{pmatrix}(r_1) \cdot \begin{pmatrix} r_2 \\ 1 \end{pmatrix}$$

this means the vectors $\begin{pmatrix} P_1 \\ P_0 \end{pmatrix}^{(j)}(r_1)$ are pairwise linearly dependent, so in particular

$$\begin{pmatrix} P_1 \\ P_0 \end{pmatrix}^{(j)}(r_1) \cdot \begin{pmatrix} -P_0 \\ P_1 \end{pmatrix}^{(j+1)}(r_1) = 0 \quad \text{for any } 0 \le j \le l-2$$

Using the chain rule for the dot product,

$$\frac{\mathrm{d}^j}{\mathrm{d}x^j}\left[\begin{pmatrix} P_1 \\ P_0 \end{pmatrix} \cdot \begin{pmatrix} -P_0' \\ P_1' \end{pmatrix}\right](r_1) = 0 \quad \text{for any } 0 \le j \le l-2$$

This dot product is a polynomial in one variable with integer coefficients, so the Gauss Lemma applies to the dot product, giving $q_1^{l-1} \le |P_1 P_0' - P_1' P_0| \le 2(\deg P)^2 |P|^2$ whenever $P_1 P_0' - P_1' P_0 \ne 0$. This then gives $|P| \ge (\sqrt{2}\deg P)^{-1} q_1^{\frac{k-1}{2}}$.

Suppose $P_1 P_0' - P_1' P_0 = 0$. Then either $P_1 = 0 \Rightarrow |P| = |P_0| \ge q_1^k$ by the Gauss lemma, which satisfies our sought after bound, or

$$\left(\frac{P_1}{P_0}\right)' = 0 \Rightarrow \exists C \in \mathbb{Q} : P_0 = C \cdot P_1 \Rightarrow P(x_1, x_2) = (x_2 + C) \cdot P_1(x_1).$$

In this latter case, we must have either $C = -r_2 = -p_2/q_2 \Rightarrow |P| \ge q_2$ or $P_1^{(j)}(r_1) = 0,\ 0 \le j \le l-1 \Rightarrow |P| \ge |P_1| \ge q_1^k$. □

Theorem 7 (Thue)**.** *Suppose β is an algebraic number of degree $d \ge 3$ and let $s \ge \frac{d+2}{2}$. Then there are at most finitely many solutions p/q in lowest terms satisfying*

$$\left|\beta - \frac{p}{q}\right| \le q^{-s}$$

Remark 8. This also implies the existence of a constant C depending only on β and s such that

$$\left|\beta - \frac{p}{q}\right| > C \cdot q^{-s}$$

for all integers p, q.

Proof. Outline: Suppose we can choose good approximations $p_1/q_1, p_2/q_2$ with arbitrarily large denominators. The proof is analogous to that of Louiville's theorem:

a) Find an auxiliary polynomial: By counting parameters, we can make sure $P \in \mathbb{Z}[x_1, x_2]$ vanishes to a high order at (β, β) while controlling the degree and norm of P.

b) Vanishing at $\frac{p}{q}$: Show that P must also vanish at $(p_1/q_1, p_2/_2)$ to high order.

c) Lower Bound: Proposition 6 gives a lower bound on $|P|$

d) Upper Bound: We get a good upper bound on $|P|$ by the construction of P.

e) Compare Bounds: The two bounds contradict each other.

□

2 Number of Solutions to Diophantine Equations

Take $P \in \mathbb{Z}[x_1, ..., x_n]$ with $\deg P = d$. We would like to estimate the number of integer solutions to the equation $P(x) = 0$. This number may be infinite, in which case we want to estimate the number of solutions of a given magnitude, i.e.:

$$\#\{x \in \mathbb{Z}^n \ : \ 2^s \leq |x| < 2^{s+1}, \ P(x) = 0\} \tag{1}$$

We have $\#\{x \in \mathbb{Z}^n \ : \ 2^s \leq |x| < 2^{s+1}\} \sim 2^{sn}$. We can make a rough guess using

$$|x| \sim 2^s \Longrightarrow |P(x)| \lesssim 2^{sd}$$

which implies that if $P(x)$ *behaves randomly*, it should be 0 about one in 2^{sd} of the time. Our estimate for 1 is therefore $\sim 2^{ns}/2^{ds}$

Guess 1. Let $P \in \mathbb{Z}[x_1, ..., x_n]$ with $\deg P = d$. If $d \leq n$, then $P(x)$ has infinitely many integer solutions, the number of such solutions of size $\sim 2^s$ is $\sim 2^{(n-d)s}$.

Guess 2. Let $P \in \mathbb{Z}[x_1, ..., x_n]$ with $\deg P = d$. If $d > n$, then $P(x)$ has at most finitely many solutions.

Both of these guesses are wrong. The equation

$$2x + 2y - 1 = 0$$

contradicts the first guess while $(x - y)^9 - 1 = 0$ contradicts the other. The second guess also has counterexamples with irreducible polynomials: The image of a

polynomial map such as $\phi(t) = (t^2 + 1, t^3 + t + 1)$ lies in the vanishing locus of an irreducible polynomial in two variables, in this case the image of ϕ is contained in the set of solutions of $x^3 - y^2 - x^2 + 2y - 1 = 0$ and, of course, any $t \in \mathbb{Z}$ gives an integer solution $\phi(t)$.

However, the following theorem, a corollary of Theorem 7, gives conditions under which Guess 2 is correct.

Theorem 9 (Thue)**.** *Let $P \in \mathbb{Z}[x, y]$ be an irreducible homogeneous polynomial of degree $d \geq 3$ and $A \in \mathbb{Z}$. The equation $P(x, y) = A$ has at most finitely many integer solutions.*

Proof. Since P is homogeneous, we can divide by y^d to get an equation $Q(x/y) = Ay^{-d}$. So for large $|y|$, we must have very small $|Q(x/y)|$. We want to show that x/y has to be very close to one of the roots β_j of Q. Suppose there are infinitely many solutions $\{(p_n, q_n) : n \in \mathbb{N}\}$, then (at least for a subsequence) $q_n \to \infty$ which implies $Q(p_n/q_n) = Aq_n^{-d} \to 0$. Factoring Q over $\mathbb{C}$ gives us

$$\lim_{n\to\infty} a\left(\frac{p_n}{q_n} - \beta_1\right)\cdots\left(\frac{p_n}{q_n} - \beta_d\right) = 0$$

For complex numbers β_j algebraic of degree d over $\mathbb{Q}$. After passing to a suitable subsequence, we find $p_n/q_n \to \beta_i$ for some i. It follows that $\beta_i \in \mathbb{R}$.

Since all the roots are distinct (Q irreducible), there exists C depending only on P such that $|p_n/q_n - \beta_j| > C^{-1}$ for all $i \neq j$ and sufficiently large n. Thus we have infinitely many (p_n, q_n) satisfying:

$$aC^{-d+1}\left|\frac{p_n}{q_n} - \beta_i\right| \leq \left|Q\left(\frac{p_n}{q_n}\right)\right| = |q_n^{-d}|A$$

A contradiction of Theorem 7. □

References

[1] Dill, G. Advanced topics in number theory: Ss 2024. Introduction to Diophantine Geometry.

[2] Guth, L. *Polynomial methods in combinatorics*, vol. 64. American Mathematical Soc., 2016.